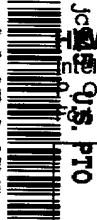


11/21/00



11-24-00
A
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10005173-1

IN THE U.S. PATENT AND TRADEMARK OFFICE
Patent Application Transmittal Letter

COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 CFR 1.53(b) is a(n): ☒ Utility ☐ Design
☒ original patent application,
☐ continuation-in-part application

jc918 U.S. PTO
09/718583
11/21/00

INVENTOR(S): John A. Bertani et al

TITLE: A Method And Apparatus For Providing An Automated Login Process

Enclosed are:

☒ The Declaration and Power of Attorney. ☒ signed ☐ unsigned or partially signed
☒ 2 sheets of drawings (one set) ☐ Associate Power of Attorney
☐ Form PTO-1449 ☒ Information Disclosure Statement and Form PTO-1449
☐ Priority document(s) ☐ (Other) _____ (fee \$ _____)

CLAIMS AS FILED BY OTHER THAN A SMALL ENTITY				
(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) TOTALS
TOTAL CLAIMS	16 — 20	0	X \$18	\$ 0
INDEPENDENT CLAIMS	3 — 3	0	X \$80	\$ 0
ANY MULTIPLE DEPENDENT CLAIMS	0		\$270	\$ 0
BASIC FEE: Design (\$320.00); Utility (\$710.00)				\$ 710
TOTAL FILING FEE				\$ 710
OTHER FEES				\$
TOTAL CHARGES TO DEPOSIT ACCOUNT				\$ 710

Charge \$ 710 to Deposit Account 08-2025. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16, 1.17, 1.19, 1.20 and 1.21. A duplicate copy of this sheet is enclosed.

"Express Mail" label no. EL712573570USDate of Deposit Nov 21, 2000

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Commissioner for Patents, Washington, D.C. 20231

By Raymond A. Jencki
Typed Name: Raymond A. Jencki

Respectfully submitted,

John A. Bertani et al

By Raymond A. Jencki
Raymond A Jencki

Attorney/Agent for Applicant(s)

Reg. No. 31,267

Date: Nov 21, 2000

Telephone No.: (541) 715-8441

5

A METHOD AND APPARATUS FOR PROVIDING AN AUTOMATED LOGIN PROCESS

Technical Field

10 The present invention relates generally to Internet electronic commerce, and in particular to registration with a web server by a user visiting the web server.

Background of The Invention

15 A typical electronic commerce (eCommerce) web site allows a consumer, logging onto the web site from a client data terminal, such as a personal computer (PC) or a workstation, to purchase goods or services offered by the company maintaining the web site. Such a web site typically requires that the consumer login with the web server that is actually hosting the site. The "login" process usually means that the consumer provide registration information, such as a name, address, telephone number, and electronic mail
20 (email) address, before the consumer is able to access the services offered by the web site. The consumer's registration information is stored in a database maintained by the host server, and in response to receiving the information the host server typically provides the consumer with a unique personal identifier, such as a personal identification number (PIN), that is associated with the stored information. When the consumer
25 subsequently revisits the web site, the PIN can serve to authenticate the user instead of requiring the user to fully re-register.

 It is not uncommon for an eCommerce web site to include one or more computer input marks, such as an icon or a textual phrase, that allows a consumer visiting the web site to connect to a second, perhaps unrelated web site hosted by a second web server.
30 Typically, when the second web site is another eCommerce web site, the consumer is again required to login at the second web site, again providing registration information and receiving, in return, a second personal identifier. When, at a future time, the

consumer again returns to the second web site via the first web site, the consumer is again required to login to the second web site, providing at least the second personal identifier if not additional registration information. Requiring the consumer to repeatedly provide extensive information every time a consumer links to an eCommerce web site via another eCommerce web site is cumbersome and inconvenient to the consumer.

In order to avoid such repetitive logins, some web servers store on a client data terminal (the consumer's PC) small data files, (also referred to as "objects") known as "cookies." When a user of a client data terminal first links to a web site, the host server obtains registration information from the consumer and stores the registration information and/or an assigned personal identifier in a cookie that is stored on the client data terminal. When the user of the client data terminal subsequently links to the web site, the host server locates the cookie on the client data terminal and retrieves the registration information and/or personal identifier from the cookie, eliminating the need for the user to again provide the information or identifier. The use of cookies by host servers has become so widespread that issues of consumer privacy and the storage of cookies on consumers' computers are topics of heated public debate. Some consumers even attempt to block the storage of cookies on their computers or disable cookies already stored there. Furthermore, cookies do not address the needs of the mobile user who often has access to computers spread over distances.

Therefore, a need exists for a method and apparatus whereby a consumer can link to a second web site through a first web site and access the services of the second web site without being required to provide registration information or a personal identifier and without the use of a "cookie."

Summary of The Invention

An automated login process is provided for a user connecting to a server, wherein the server is a first server of multiple servers that are connected via a computer network.

The server receives a connection to the user via a client data terminal, receives an identifier associated with a second server of the multiple servers, and authenticates the user based on the identifier. By authenticating the user based on the identifier, the need for the user to input registration information or a personal identifier as part of the login process is eliminated.

Brief Description of the Drawings

FIG. 1 is a block diagram of a computer data system in accordance with the present invention.

5 FIG. 2 is a logic flow diagram of the steps executed by a web server in providing an automated login process in accordance with the present invention.

Detailed Description of the Invention

10 The present invention can be more fully understood with reference to FIGs. 1 and 2. FIG. 1 is a block diagram of a computer data system 100 in accordance with the present invention. A user at a client data terminal 102, such as a personal computer or a workstation, accesses each of multiple web servers 110, 114 (two shown) via a data network 108 such as the Internet. Each of web servers 110, 114 can be an HP 9000 K-series server or an HP 9000 Enterprise server available from Hewlett-Packard Company or any other web server or equivalent thereof, including for example, a network of computers or processors that are linked together, which is known art. Each of the web servers 110, 114 is typically operated by, or at the behest of, a provider of goods or services and includes a registration system whereby a prospective purchaser of goods or services, or a previous customer (all of which are hereinafter referred to as a "user") connects to the server and registers with the server and whereby the server authenticates the user upon subsequent visits by the user to the server. Each web server 110, 114 stores one or more user interfaces, such as a web page, in a memory associated with the server. Each user interface provides a means by which a server 110, 114 can exchange information with the user when the user is connected to the server via client data terminal 102.

25 Client data terminal 102 includes a processor 104 coupled to a memory 106 that stores instructions and programs, including a web browser application, that are executed by the processor. A user of client data terminal 102 establishes a connection to a web server 110, 114 by activating the web browser stored in memory 106 and inputting a uniform resource locator (URL) corresponding to an Internet Protocol (IP) address of a web server 110, 114. Using known techniques and communication protocols, the web browser then connects, via data network 108, with the web server corresponding to the

input URL. Many other methods are known for instructing a web browser to connect a client data terminal to a web server and may be used herein without departing from the spirit and scope of the present invention.

When a user of client data terminal 102 connects to a web server, such as web
5 server 110, the user is typically requested by the web server to "login." The login
process typically requires that the user provide to the server (i.e., server 110) registration
information, such as the user's name, post office address, telephone number, and
electronic mail (email) address, or provide a personal identifier by which server 110 can
authenticate the user. In one embodiment of the present invention, when the user
10 connects to server 110, the server conveys to the user, via client data terminal 102, a user
interface. Included in the user interface is a request that the user login, that is, provide
a personal identifier or registration information, and appropriate data fields for the input
of the requested information. The user then inputs the appropriate data into the
appropriate data fields and conveys the data back to server 110. When the data then
15 received by server 110 includes registration information, server 110 stores the received
data, preferably in a user profile that server 110 creates in a registration database 112 that
is included in or connected to the server.

Upon receiving registration information from the client data terminal, server 110
generates a personal identifier that typically includes one or more symbols or
20 alphanumeric values, such as a personal identification number (PIN) or password, that
is associated with the registration information just received by server 110 from the user.
Alternative embodiments might generate personal identifiers that are comprised of other
combinations of words, phrases or the like. Server 110 stores the personal identifier,
preferably in the user's profile, which is a data file in registration database 112, and
25 conveys the personal identifier to the user. Use of the personal identifier thereafter
allows the user to expedite the login process when the user subsequently connects to
server 110, wherein the user need only provide the personal identifier to server 110
instead of again providing registration information. Upon receiving the personal
identifier from the user during such subsequent connections, server 110 then
30 authenticates the user by searching for, and locating, a matching personal identifier in
registration database 112. A match between a stored personal identifier and the personal
identifier sent to the server 110 by a putative user, provides a basis for the server to

consider the user who supplied the personal identifier to be the same person to whom the personal identifier was first supplied and identified by the data that the user provided during the registration process. By way of a personal identifier match, the user is considered to be authenticated.

5 In the present invention, included in one of the one or more user interfaces of web server 110 is a computer input mark, such as an icon or a textual phrase, that includes a hyperlink to a second web server, such as web server 114. Selection of the computer input mark by the user causes the web browser running on client data terminal 102 to establish a connection to the second web server, that is, server 114. Web server 110 is
10 affiliated with web server 114 in the sense that web server 110 provides a means by which a user visiting web server 110 can connect to web server 114. In the prior art, in the absence of a "cookie," each time the user connects to server 114 via the hyperlink of server 110, the user is required to login to server 114 by providing either registration information or a personal identifier. The present invention eliminates the need for the
15 user to provide any login information when connecting to server 114 via the hyperlink of server 110 after going through a one-time registration process.

Computer input marks are well known in the art. Computer input marks typically include an underlying URL associated with another file in the web server or with a file in another web server. Computer input marks typically further include an underlying
20 instruction, executed by a web browser running on a client data terminal, to establish a connection between the client terminal and the server and file associated with the underlying URL. In one embodiment of the present invention, the computer input mark of the user interface of web server 110 further includes an underlying personal identifier, which personal identifier was assigned to the user by web server 110, and an underlying
25 provider identifier associated with web server 110. The provider identifier allows the web server associated with the underlying URL, that is, web server 114, to identify the affiliated web server that served as the source of the hyperlink, that is, web server 110.

When the user of client data terminal 102 selects the computer input mark of the user interface of web server 110, processor 104 of client data terminal 102 establishes a
30 connection between the terminal and server 114 via data network 108, and conveys to server 114 the personal identifier and the provider identifier associated with server 110.

When the user of client data terminal 102 selects the computer input mark of the user interface of web server 110, processor 104 of client data terminal 102 establishes a connection between the terminal and server 114 via data network 108, and conveys to server 114 the user identifier associated with server 110.

30

After the user leaves web server 114, the present invention provides a transparent login process for the user when he or she subsequently reconnects to web server 114 via the computer input mark included in the user interface of web server 110. When the user subsequently reconnects to server 114 via the computer input mark, server 114 again

receives from client data terminal 102 the personal identifier and provider identifier that underlie the computer input mark. Server 114 then searches registration database 116 for a personal identifier and provider identifier that match the received identifiers, which matching identifiers are stored in the user's profile. Upon locating the previously stored, matching identifiers, server 114 authenticates the user and permits the user access to one or more services provided by the server. Server 114 can also retrieve, from database 116, the user's stored registration information and personal identifier generated by server 114 based on the personal identifier and provider identifier conveyed by terminal 102.

For example, and merely for the purpose of illustrating the principles of the present invention, suppose that server 110 generates, and conveys to a user, a personal identifier 'X' when the user first registers with the server. A computer input mark of a user interface of server 110 includes a hyperlink to server 114 and further includes the personal identifier 'X' and a provider identifier 'Y' that is uniquely associated by server 114 with server 110. When the user then connects to server 114 via the computer input mark of server 110, the user's client data terminal 102 conveys to server 114 the personal identifier 'X' and the provider identifier 'Y.' Server 114 then requests and receives registration information from the user and stores the registration information, along with the personal identifier 'X' and the provider identifier 'Y,' in a profile of the user in registration database 116. Server 114 also generates a personal identifier 'Z' that is also stored in the user's profile in database 116.

The next time that the user connects to server 114 via the computer input mark of server 110, the user's client data terminal 102 again conveys to server 114 the personal identifier 'X' and the provider identifier 'Y.' Upon receiving the reconveyed identifiers 'X' and 'Y,' server 114 searches registration database 116 for a stored 'X' and a corresponding stored 'Y.' Upon locating the stored 'X' and 'Y' in the user's profile in database 116, server 114 authenticates the user and permits the user access to one or more services provided by server 114.

By authenticating the user based on the personal identifier and provider identifier conveyed to server 114 by client data terminal 102, the present invention eliminates the need for the user to provide any data when logging onto server 114 after going through a one-time registration process. System 100 thereby presents the user with a seamless transition from server 110 to server 114, eliminating any need for the user to stop and

provide any login information such as registration information or a personal identifier.

FIG. 2 is a logic flow diagram 200 of a method for providing automated registration for a user connecting to a server, wherein the server comprises a first server of multiple servers that are connected via a computer network. The method starts (201) when the first server receives (202) a connection from the user for a first time. In the present invention, the connection is established as a result of the user selecting a computer input mark of a second server of the multiple servers, which computer input mark includes a hyperlink to the first server. Upon receiving the connection, the first server requests that the user to login. As a part of the login process, the first server receives (203) an identifier associated with the second server, which identifier preferably identifies both the user and the second server. Alternatively, the server may receive both a provider identifier associated with the second server and a personal identifier assigned to the user by the second server. The first server further receives (204) registration information from the user. The first server then stores (205) the received identifier and the registration information, preferably in a user profile that the first server creates in an associated registration database.

Subsequent, in time, to receiving and storing the identifier and the registration information provided by the user, the first server receives (206) a second connection with the user as a result of the user again selecting the computer input mark of the second server. Upon receiving the second connection, the first server further receives (207) the identifier associated with the second server, or alternatively receives both the provider identifier associated with the second server and the personal identifier assigned to the user by the second server. The first server then authenticates (208) the user based on the identifier, preferably by locating a matching identifier that was previously stored in the registration database, and the logic flow ends (209). Preferably the step of authentication (208) includes the steps of authenticating the user based on the identifier and allowing a user access to a service provided by the first server.

In sum, the present invention provides an automated login process for a user logging onto a host server via an affiliated server. When the user first logs onto the host server via the affiliated server, the host server is provided, by the user's client data terminal, a provider identifier and a personal identifier associated with the affiliated

server. The provider identifier and the personal identifier are then stored by the host server in a registration database associated with the host server, along with registration information provided by the user. When the user subsequently connects to the host server via the affiliated server, the user's client data terminal again provides the provider identifier and personal identifier to the host server. The host server is then able to authenticate the user by matching the received provider identifier and personal identifier with the provider identifier and personal identifier stored in the registration database, without requiring any data to be input by the user. By eliminating the need for the user to input any data, the present invention provides a login process that is seamless and transparent to the user, yet does not use a cookie.

While the present invention has been particularly shown and described with reference to particular embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the present invention.

What is claimed is:

- 1 1. A method for providing an automated login for a user connecting to a server,
2 wherein the server comprises a first server of a plurality of servers that are connected via
3 a computer network, the method comprising steps of:
4 receiving a connection to the user via a client data terminal;
5 receiving an identifier associated with a second server of the plurality of servers;
6 and
7 authenticating the user based on the identifier.
- 1 2. The method of claim 1, wherein the identifier comprises a provider identifier
2 associated with the second server and a personal identifier assigned to the user by the
3 second server.
- 1 3. The method of claim 1, wherein the step of authenticating the user comprises a
2 step of allowing a user access to a service provided by the first server.
- 1 4. The method of claim 1, wherein the step of receiving a connection comprises a
2 step of receiving a second connection to a user via a client data terminal, wherein the step
3 of receiving a provider identifier comprises a step of receiving, during the second
4 connection, a provider identifier associated with a second server of the plurality of
5 servers, wherein the step of receiving a personal identifier comprises a step of receiving,
6 during the second connection, a personal identifier assigned to the user by the second
7 server, and further comprising steps of:
8 receiving a first connection to the user via a client data terminal, wherein the first
9 connection is first in time relative to the second connection;
10 receiving, during the first connection, an identifier associated with the second
11 server;
12 receiving registration information from the user;
13 storing the identifier and the registration information; and
14 wherein the step of authenticating the user comprises a step of matching the
15 stored identifier with the identifier received during the second connection.

1 5. The method of claim 4, wherein the identifier received during the first connection
2 and the identifier received during the second connection each comprises a provider
3 identifier associated with a second server and a personal identifier assigned to the user
4 by the second server.

1 6. The method of claim 4, wherein the step of storing comprises steps of:
2 creating a user profile; and
3 storing the identifier and the registration information in the user profile.

1 7. The method of claim 4, further including steps of:
2 requesting, during the first connection, a consent of the user to use the identifier
3 associated with the second server; and
4 receiving the requested consent.

1 8. The method of claim 1, wherein the registration information comprises at least
2 one of a user name, user post office address, user telephone number, and user electronic
3 mail address.

1 9. The method of claim 1, further comprising a step of assigning, by the first server
2 and during the first connection, a personal identifier to the user.

1 10. A method for providing an automated login for a user logging onto a host web
2 site, the method comprising steps of:
3 receiving a connection to a user via an affiliated web site;
4 receiving an identifier associated with the affiliated web site; and
5 allowing the user access to the host web site based on the received identifier.

1 11. The method of claim 10, wherein the identifier comprises a provider identifier
2 associated with the affiliated web site and a personal identifier assigned to the user by a
3 server hosting the affiliated web site.

1 12. The method of step 10, wherein the step of receiving a connection comprises a

09713583.1 2/10/00

2 step of receiving a second connection of a user via an affiliated web site, wherein the step
3 of receiving an identifier comprises a step of receiving, during the second connection, an
4 identifier associated with the affiliated web site, and further comprising steps of:

5 receiving a first connection of the user via the affiliated web site, wherein the first
6 connection is first in time relative to the second connection;

7 receiving, with respect to the first connection, registration information from the
8 user;

9 receiving, with respect to the first connection, an identifier associated with the
10 affiliated web site; and

11 storing the registration information and identifier received with respect to the first
12 connection.

1 13. The method of claim 12, wherein the identifier received during the first
2 connection and the identifier received during the second connection each comprises a
3 provider identifier associated with the affiliated web site and a personal identifier
4 assigned to the user by the affiliated web site.

1 14. The method of claim 12, wherein the registration information and identifier
2 received with respect to the first connection is stored in a database, and wherein the step
3 of allowing comprises steps of:

4 searching the database for an identifier that matches the identifier received with
5 respect to the second connection; and

6 when a matching identifier is located, allowing the user access to the host web
7 site.

1 15. A server comprising:

2 a means for receiving a first connection and a second connection to a client data
3 terminal, wherein the first connection is first in time relative to the second connection;

4 a means for receiving registration information during the first connection from
5 a user of the client data terminal;

6 a means for receiving an identifier associated with an affiliated server during the
7 first connection, which affiliated server was visited by the user prior to the server

1 16. The server of claim 15, wherein the identifier received during the first connection
2 and the identifier received during the second connection each comprises a provider
3 identifier associated with the affiliated server and a personal identifier assigned to the
4 user by the affiliated server.

Abstract of the Disclosure

An automated login process is provided for a user connecting to a first server of multiple servers that are connected via a computer network. The server receives a connection to the user via a client data terminal, receives an identifier associated with a second server of the multiple servers, and authenticates the user based on the identifier.

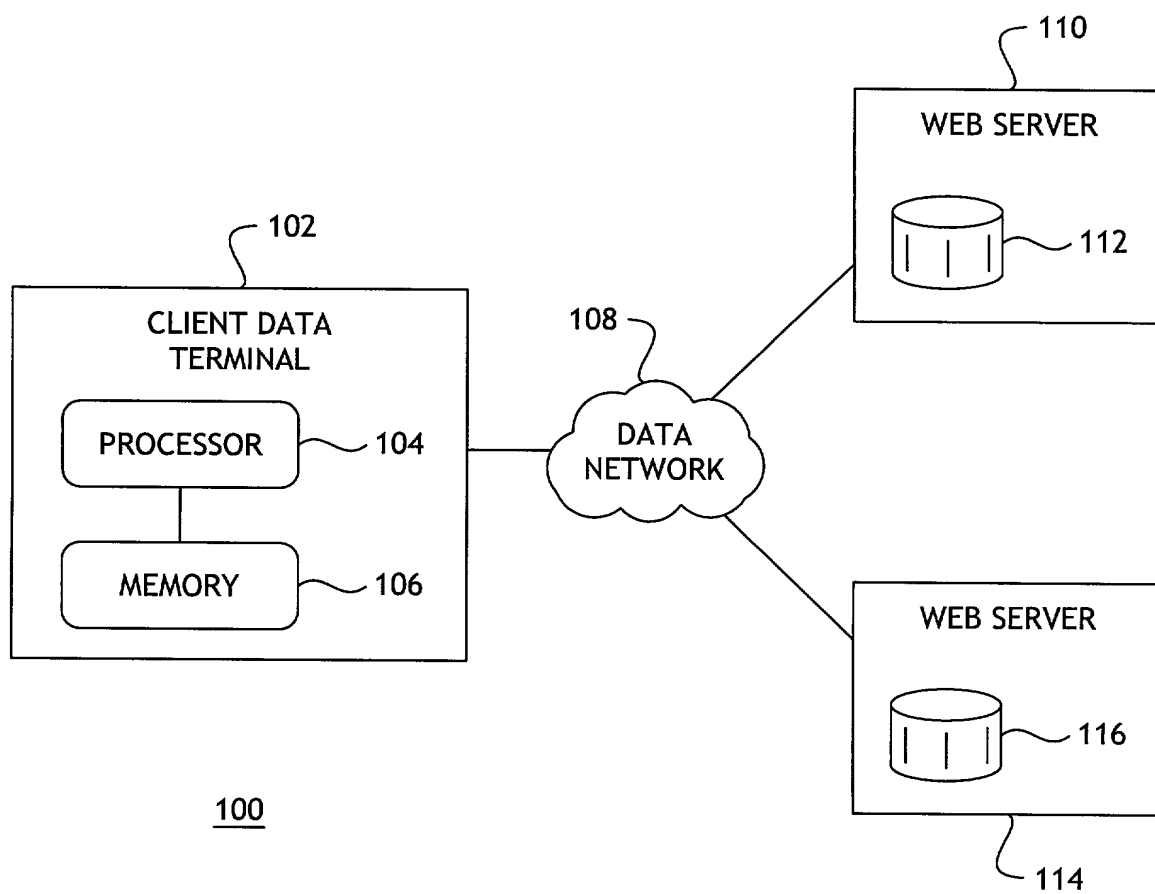


Fig. 1

Fig. 2

DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATIONATTORNEY DOCKET NO. 10005173-1

As a below named inventor, I hereby declare that:

My residence/post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

A Method And Apparatus For Providing An Automated Login Process

the specification of which is attached hereto unless the following box is checked:

() was filed on _____ as US Application Serial No. or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

Foreign Application(s) and/or Claim of Foreign Priority

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor(s) certificate listed below and have also identified below any foreign application for patent or inventor(s) certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE FILED	PRIORITY CLAIMED UNDER 35 U.S.C. 119
			YES: _____ NO: _____
			YES: _____ NO: _____

Provisional Application

I hereby claim the benefit under Title 35, United States Code Section 119(e) of any United States provisional application(s) listed below:

APPLICATION SERIAL NUMBER	FILING DATE

U. S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (patented/pending/abandoned)

POWER OF ATTORNEY:

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

Customer Number **022879**Place Customer
Number Bar Code
Label hereSend Correspondence to:
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400**Direct Telephone Calls To:**Raymond A Jenski
(541) 715-8441

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Inventor: John A. Bertani Citizenship: USResidence: 1181 NW ^{Country} Court Corvallis OR 97330Post Office Address: Same as residence

Inventor's Signature

Date

11-16-2000

**DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION (continued)**

ATTORNEY DOCKET NO. 10005173-1

Full Name of # 2 joint inventor: John M. Kerr Citizenship: US

Residence: 2982 NW Pineview Albany OR 97321

Post Office Address: Same as residence

John M. Kerr Inventor's Signature Date 16 Nov 2000

Full Name of # 3 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature Date

Full Name of # 4 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature Date

Full Name of # 5 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature Date

Full Name of # 6 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature Date

Full Name of # 7 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature Date

Full Name of # 8 joint inventor: _____ Citizenship: _____

Residence: _____

Post Office Address: _____

Inventor's Signature Date

00737 633760